UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/419,828	10/14/1999	DON VAN DYKE	M-7084-US	1859

23418 7590 05/03/2006

VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
SMITHERS, MATTHEW	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/419,828	DYKE ET AL.	
	Examiner	Art Unit	
	Matthew B. Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-13 and 15-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-13 and 15-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114 was filed in this application after appeal to the Board of Patent Appeals and Interferences, but prior to a decision on the appeal. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on February 21, 2006 has been entered.

Response to Arguments

Applicant's arguments, see amendment, filed February 21, 2006, with respect to the rejection(s) of claim(s) 1, 3-13, 15-23 under 35 USC 102(e) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Orenstein et al (US patent 5,787,026) in view of Boyle (US patent 6,118,870) and Schneier's Applied Cryptography.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-13 and 15-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orenstein et al (US patent 5,787,026) in view of Boyle (US patent 6,118,870) and Schneier's Applied Cryptography.

Regarding claims 1, 3, 4, 5, 6, 7, 10, 11, and 12, Orenstein teaches pipeline processing using a Pentium processor that includes an arithmetic logic unit (ALU) and registers for processing instructions and data (see column 1, line 45 to column 2, line 20). The ALU receives operands from a register file and performs the instructions associated with the operands (see column 1, line 65 to column 2, line 20; column 6, line 52 to column 7, line 7 and column 10, lines 48-65). Further, Orenstein teaches the multimedia pipeline is not only applicable to specialized applications but can also apply to general purpose computers (see column 7, lines 30-37). Orenstein fails to specifically teach an embodiment where the Pentium processor performs DES operations on the multimedia data. Boyle teaches a microprocessor (off-the-shelf Pentium) having instruction set extensions for performing DES operations on multimedia data (see column 5, lines 14-31; column 6, line 66 to column 7, line 15 and column 8, lines 43-48). Boyle fails to specifically teach the processing steps of the DES algorithm. Schneier is being relied on for further illustrating the processing steps of the DES algorithm, which is old and well known, but silent in Boyle's teaching. Schneier clearly teaches applying the DES algorithm to a 64-bit block of plaintext (datum) using a 48-bit key (subkey) selected from a 56-bit key (see page 270, "Description of DES" and "Outline of the

Algorithm" (DES operates on a 64-bit block of plaintext. . . In each round . . . 48 bit are selected from the 56 bits of the key and further teaches an expansion permutation, S-box substitution, P-box permutation and associated XOR operations steps being performed in the DES processing (see page 270-271, "Outline of the Algorithm", page 373, Figure 12.2, page 273, "The Expansion Permutation", page 274-275, "S-box Substitution", page 275-277, "The P-box Permutation"). The 64-bit block of plaintext is divided into a right half (R_i's) consisting of 32-bits and a left half consisting of 32-bits (L_i's) (see page 270, "Outline of the Algorithm" (. . . the block is broken into a right half and a left half, each 32 bits long. . .). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Schneier's description of how DES works and Boyle's instruction set extensions for multimedia applications with Orenstein's apparatus for pipeline processing of multimedia data for the purpose of protecting the multimedia data as it undergoes processing by the Pentium processor. One of ordinary skill in the art would have been motivated to combine Boyle with Orenstein in order to prevent a pirate from unauthorized access and use of compressed multimedia data [see Boyle et al; column 1, line 61 to column 2, line 2].

Regarding claims 8 and 9, Orenstein as modified teaches a bypass mechanism provided in the register file (see column 8, lines 10-33; column 10, lines 43-45; column 11, lines 41-46; and Figure 3A.

Regarding claims 13, 15, 16, 17, 18, 19, 20 and 21, Orenstein teaches pipeline processing using a Pentium processor that includes an arithmetic logic unit (ALU) and registers for processing instructions and data (see column 1, line 45 to column 2, line

20). The ALU receives operands from a register file and performs the instructions associated with the operands (see column 1, line 65 to column 2, line 20; column 6, line 52 to column 7, line 7 and column 10, lines 48-65). Further, Orenstein teaches the multimedia pipeline is not only applicable to specialized applications but can also apply to general purpose computers (see column 7, lines 30-37). Orenstein fails to specifically teach an embodiment where the Pentium processor performs DES operations on the multimedia data. Boyle teaches a microprocessor (off-the-shelf Pentium) having instruction set extensions for performing DES operations on multimedia data (see column 5, lines 14-31; column 6, line 66 to column 7, line 15 and column 8, lines 43-48). Boyle fails to specifically teach the processing steps of the DES algorithm. Schneier is being relied on for further illustrating the processing steps of the DES algorithm, which is old and well known, but silent in Boyle's teaching. Schneier clearly teaches applying the DES algorithm to a 64-bit block of plaintext (datum) using a 48-bit key (subkey) selected from a 56-bit key (see page 270, "Description of DES" and "Outline of the Algorithm" (DES operates on a 64-bit block of plaintext. . . In each round . . . 48 bit are selected from the 56 bits of the key and further teaches an expansion permutation, S-box substitution, P-box permutation and associated XOR operations steps being performed in the DES processing (see page 270-271, "Outline of the Algorithm", page 373, Figure 12.2, page 273, "The Expansion Permutation", page 274-275, "S-box Substitution", page 275-277, "The P-box Permutation"). The 64-bit block of plaintext is divided into a right half (R_i's) consisting of 32-bits and a left half consisting of 32-bits (L_i's) (see page 270, "Outline of the Algorithm" (. . . the block is broken into a right half

and a left half, each 32 bits long. . .). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Schneier's description of how DES works and Boyle's instruction set extensions for multimedia applications with Orenstein's apparatus for pipeline processing of multimedia data for the purpose of protecting the multimedia data as it undergoes processing by the Pentium processor. One of ordinary skill in the art would have been motivated to combine Boyle with Orenstein in order to prevent a pirate from unauthorized access and use of compressed multimedia data [see Boyle et al; column 1, line 61 to column 2, line 2].

Regarding claims 22 and 23, Orenstein teaches pipeline processing using a Pentium processor that includes an arithmetic logic unit (ALU) and registers for processing instructions and data (see column 1, line 45 to column 2, line 20). The ALU receives operands from a register file and performs the instructions associated with the operands (see column 1, line 65 to column 2, line 20; column 6, line 52 to column 7, line 7 and column 10, lines 48-65). Further, Orenstein teaches the multimedia pipeline is not only applicable to specialized applications but can also apply to general purpose computers (see column 7, lines 30-37). Orenstein fails to specifically teach an embodiment where the Pentium processor performs DES operations on the multimedia data. Boyle teaches a microprocessor (off-the-shelf Pentium) having instruction set extensions for performing DES operations on multimedia data (see column 5, lines 14-31; column 6, line 66 to column 7, line 15 and column 8, lines 43-48). Boyle fails to specifically teach the processing steps of the DES algorithm. Schneier is being relied on for further illustrating the processing steps of the DES algorithm, which is old and well

known, but silent in Boyle's teaching. Schneier clearly teaches applying the DES algorithm to a 64-bit block of plaintext (datum) using a 48-bit key (subkey) selected from a 56-bit key (see page 270, "Description of DES" and "Outline of the Algorithm" (DES operates on a 64-bit block of plaintext. . . In each round . . . 48 bit are selected from the 56 bits of the key and further teaches an expansion permutation, S-box substitution, P-box permutation and associated XOR operations steps being performed in the DES processing (see page 270-271, "Outline of the Algorithm", page 373, Figure 12.2, page 273, "The Expansion Permutation", page 274-275, "S-box Substitution", page 275-277, "The P-box Permutation"). The 64-bit block of plaintext is divided into a right half (R_i's) consisting of 32-bits and a left half consisting of 32-bits (L_i's) (see page 270, "Outline of the Algorithm" (. . . the block is broken into a right half and a left half, each 32 bits long. . .). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Schneier's description of how DES works and Boyle's instruction set extensions for multimedia applications with Orenstein's apparatus for pipeline processing of multimedia data for the purpose of protecting the multimedia data as it undergoes processing by the Pentium processor. One of ordinary skill in the art would have been motivated to combine Boyle with Orenstein in order to prevent a pirate from unauthorized access and use of compressed multimedia data [see Boyle et al; column 1, line 61 to column 2, line 2].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137